IN THE CLAIMS

The following is a complete, marked up listing of revised claims with a status identifier in parentheses, underlined text indicating insertions, and strikethrough and/or double-bracketed text indicating deletions.

LISTING OF CLAIMS

1. - 16. (Canceled)

17. (Currently Amended) A method for verifying validity of a network key in a digital domestic network, communicating with at least a broadcasting device and at least one processing device, the broadcasting device having encrypted data to broadcast to the processing device, the method comprising:

providing the encrypted data accessible by the processing device due to a network key unknown by the broadcasting device;

transmitting by the broadcasting device a test key to the processing device,

receiving from the processing device a cryptogram made up of the test key encrypted by the network key, and

determining the validity of the network key by comparing the received cryptogram with at least one of a plurality of control cryptograms taken from a list of control data generated by a verification center for the test key,

wherein the control cryptograms are in a black list containing cryptograms obtained by encrypting the test key with invalid network keys [[and]] or in a white list containing the cryptograms obtained by encrypting the test key with valid network keys.

18. (Previously Presented) The method according to claim 17, wherein the test key and the control cryptograms are generated by the verification center and transferred to the broadcasting device.

19. (Cancelled)

20. (Previously Presented) The method according to claim 17, wherein the test key is randomly generated by the broadcasting device and used as session key for the encryption of the encrypted data.

21. (Previously Presented) The method according to claim 20, wherein the broadcasting device generates at least two test keys and transmits the at least two test keys to the processing device, received from the processing device the corresponding cryptograms, selects one control cryptogram from the list of control data and the associated test key for the verification operations and another control cryptogram and the associated test key as session key for the encryption of the data encryption.

22. (Canceled)

23. (Canceled)

24. (Previously Presented) The method according to claim 17, wherein an error signalization inviting the user to change the terminal module is generated when a received cryptogram is present in the black list and refused during the comparison.

25. (Previously Presented) The method according to claim 17, wherein the broadcasting device comprises a converter module in charge of the verification operations.

26. (Previously Presented) The method according to claim 17, wherein the processing device comprises a terminal module storing the network key.

27. (Previously Presented) The method according to claim 28, wherein the control cryptograms are stored in a memory of the broadcasting device, and the comparison with the received cryptogram is carried out by the broadcasting device.

28. (Previously Presented) The method according to claim 17, wherein the control data includes an address indicating where the control cryptograms can be downloaded via Internet by the broadcasting device, the control cryptograms being stored in the memory of the broadcasting device.

29. (Previously Presented) The method according to claim 28 wherein the converter module verifies the authenticity of the list of control data via a signature on the data.

30. (Previously Presented) The method according to claim 17, wherein the control data is generated in the verification center, the broadcasting device transmits the received control cryptogram and the locally generated test key to the verification center for carrying out the verification.

31. (Previously Presented) The method according to claim 17, wherein the broadcasting device is a DVD disc reader for reading a disk, the disc includes at least one of the encrypted data and the list of control data.

32. (Previously Presented) The method according to claim 17, wherein the broadcasting device is a pay television decoder receiving the encrypted data and the list of control data from a managing center.

33. (Previously Presented) The method according to claim 17, wherein an error signalization inviting the user to change the terminal module is generated when a received cryptogram is absent of the white list and refused during the comparison.

34. (Canceled)

35. (Previously Presented) The method according to claim 26, wherein an error signalization inviting the user to change the terminal module is generated when a received cryptogram is present in the black list or absent of the white list, the received cryptogram being refused during the comparison.

36. (Previously Presented) The method according to claim 17 wherein the list of control data is generated in the verification center, the broadcasting device transmits the received control cryptogram generated by the processing device based on the test key received by the broadcasting device from the verification center, the verification center carrying out the verification.